



Cisco
mConcierge

BYOD Insights 2013: A Cisco Partner Network Study

March 2013

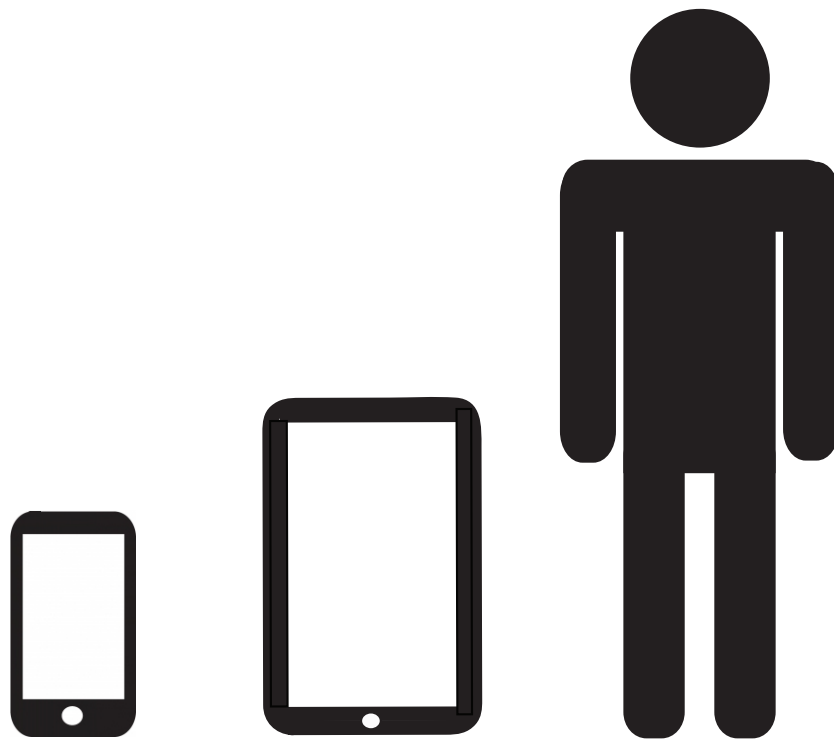


Table of Contents

National Findings.....4

Industry Findings.....6

Security.....7

Sensitive Industries.....9

Conclusions.....10

City Appendix.....11

AT A GLANCE

Millions of American workers are setting up the office wherever and whenever they can find an internet connection. And with access to an ever-widening range of devices -- smartphones, tablets and laptops -- workers aren't limiting themselves to company-provided hardware.

But what devices do they use and who owns them? Are workers being reimbursed, and if so, for how much? Are there security risks?

While experts have analyzed and parsed responses from thousands of managers, IT workers and CIOs about this "Bring Your Own Device" trend, no one's asked the everyday employee how they use their smartphones for work.

Until now. The findings of this study, commissioned by a group of Cisco partner firms, answers the types of questions thousands of managers and IT pros haven't yet asked. The findings are revealing and the landscape is startlingly different than anyone might've expected.

BYOD in the USA

Decades ago, workers lugged their own lunch pails and tools to work each morning. Later, workers might have taken their favorite calculator. Today's modern employee is transporting somewhat more advanced technology (and more of it) from home to office.

In fact, according to a recent study conducted by a group of Cisco partner firms, 90% of full-time American workers use their personal smartphones for work purposes. It's a staggering finding that validates a trend industry experts have been debating for several years now: Bring Your Own Device or BYOD. The consumerization of this technology has given the modern worker enormous work flexibility, while giving IT departments substantial headaches.

Not only are workers using their own technology for work, many are doing it frequently. 92% of BYODers access their own smartphone for work every week (62% at least every day and 30% at least once per week).

How much work are employees doing on their phones? The answer: a lot. That work might include: answering work emails; interacting with work related mobile and Web apps; and making work calls.

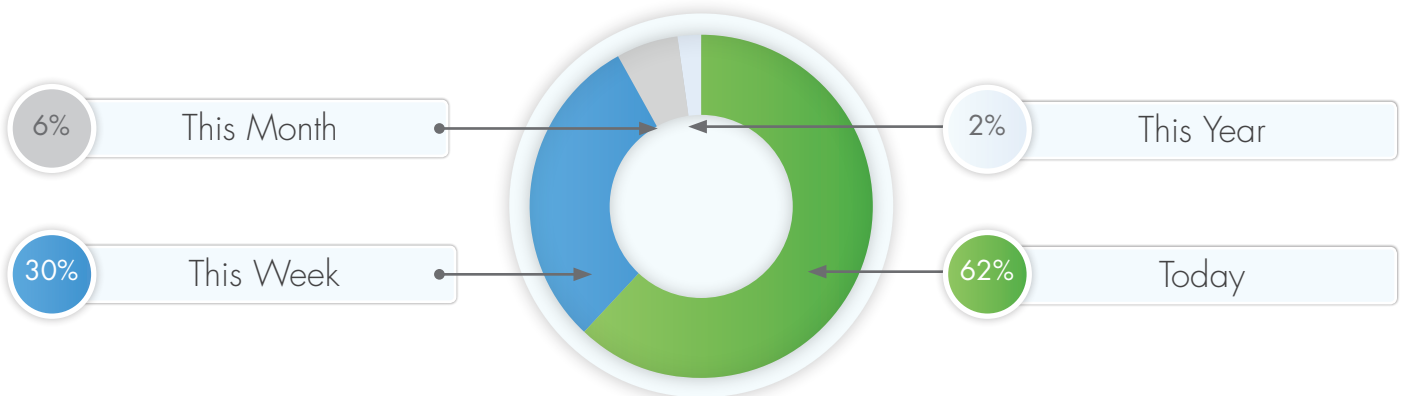
Workers aren't really clocking out either. Seventy percent of employees who use their smartphones for work are expected to read emails after working hours.

QUICK HITS

- 62% of U.S. employees who use their own smartphone for work do so everyday
- 92% of U.S. employees who use their smartphones for work did so this week
- Only 1 in 10 workers get some kind of work stipend for their smartphone
- 39% of workers who use personal smartphones for work don't password protect
- 52% access unsecured wifi networks
- 69% of BYODers are expected to access work emails after hours

92% of BYODers worked from their smartphone this week

The vast majority of American workers use their personal smartphones for work. Almost all do at least once every week.



When was the last time you used your personal smartphone for work purposes?

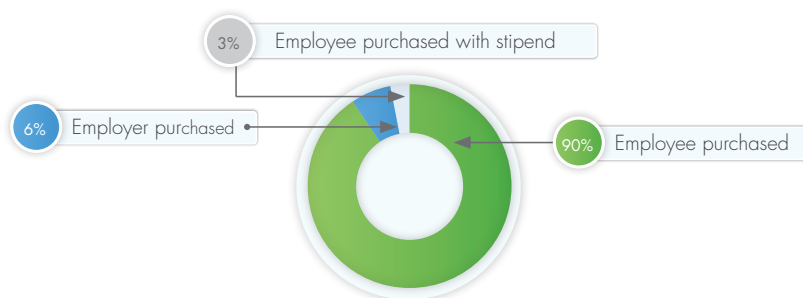
BYOD in the USA

Not many workers being reimbursed

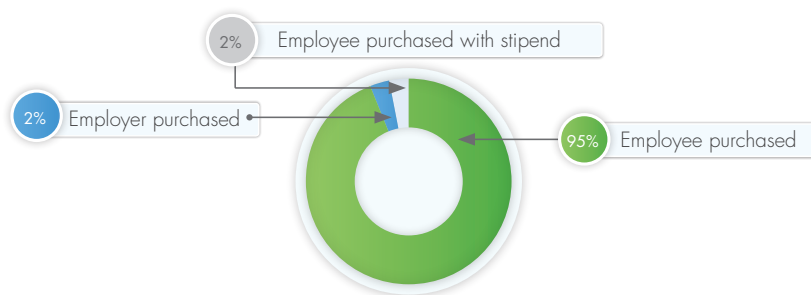
Another interesting find: employers aren't exactly rushing to compensate workers for tossing their smartphones onto the pile of capital. 90% of Americans who use their own smartphones for work (BringYourOwnDeviders) don't receive any sort of stipend or allowance to pay for a smartphone, even if they use it for work.

Only 6 percent of workers say their employers paid for their smartphones outright. Just 3 percent received a stipend. A small number of workers – 11 percent – reported receiving any kind of small reimbursement for their smartphone devices.

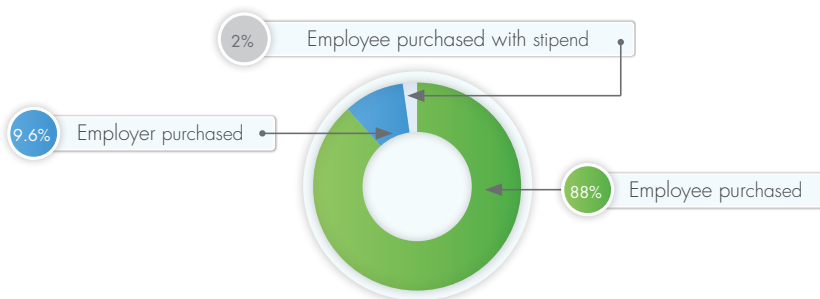
National Average



Small Business BYODers (1-24 employees)



Large Businesses BYODers (500+ employees)



BYOD by industry

Company size plays a large part in determining work/life expectations, as well as smartphone use. Smaller firms tend to expect workers to answer emails after hours more often. They also are less likely to reimburse or offer stipends for smartphones. Of workers at firms of between 1 and 25 employees, 66 percent say they're expected to read emails after working hours. That's compared with 53 percent of workers at firms of over 500 employees.

Whether you use your smartphone does vary depending on your job. Teachers are most likely to use their smartphones for work. Here's a breakdown of BYOD practices in 8 common industries.

Do you use your smartphone for work purposes?		
	Yes	No
Banking	83.3%	16.7%
Education	95.2%	4.8%
Foodservice/hospitality	80.4%	19.5%
Healthcare	88.6%	11.5%
Legal	78.6%	21.4%
Manufacturing	80.7%	19.4%
Retail/wholesale	77.1%	22.8%
Technology	90.4%	9.6%

“

70 percent of workers in the banking industry use their own smartphones for work every day

Security

Likely the most troubling finding of the study for employers is that workers who use their smartphones for work have inconsistent security habits.

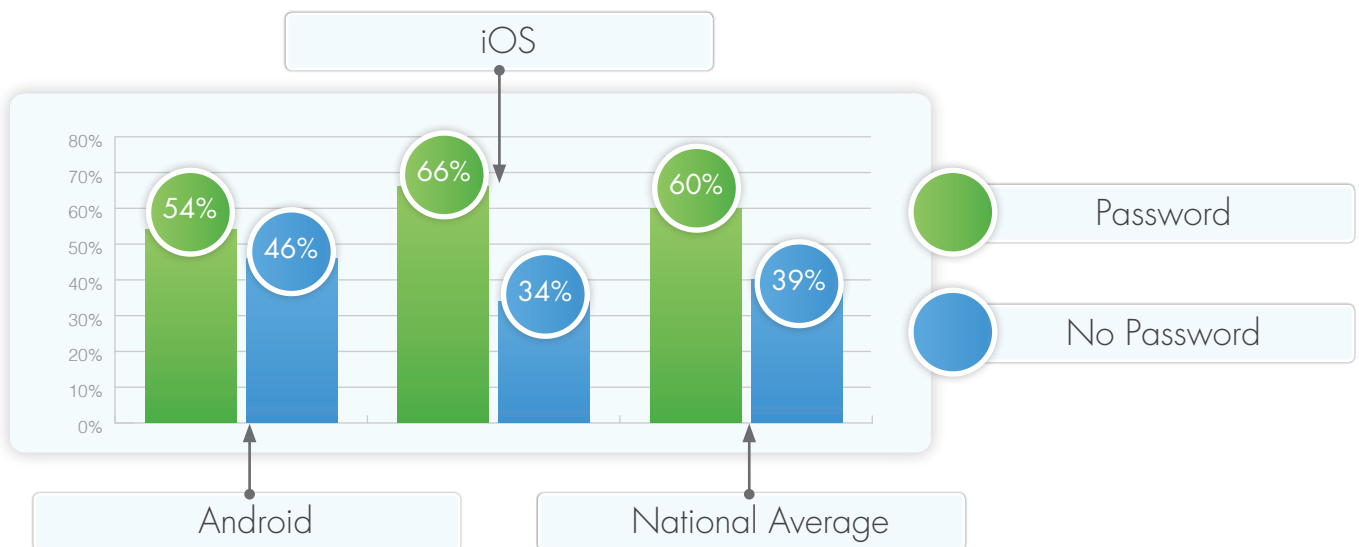
Nearly 40% of BYODers don't protect their phones with a password. So many smartphone owners are using their devices for work, yet 2 out of 5 haven't applied the most basic security protocols.

Arguably just as troubling: Fifty-two percent reported accessing unsecured wi-fi networks with their devices – a well-known vulnerability in the cybersecurity industry. Just last year a popular Mozilla Firefox plug-in was identified that allowed users to exploit devices that were connected to unsecured wi-fi networks.

Among password protectors, there seems to be a counterintuitive breakdown between operating systems. Fifty-four percent of Android users lock their devices with a password, while 66% of iOS users have password protection. As Android has carved out a larger market share, 53% worldwide according to Gartner, it may be grabbing a broader spectrum of customers, including a less sophisticated user set.

iOS users most cautious with passwords

Is your smartphone password protected?



Security

But the security issues go deeper than password protections and wi-fi access. A large number of BYODers don't even consider that their phones' Bluetooth discoverable modes may still be on; 48 percent of work smartphone users haven't disabled the feature on their devices.

According to Symantec, "When a Bluetooth device is discoverable, it is very easy to scan for it using a PC and download private data... This approach can easily contribute to some high profile attacks on celebrities and famous people, who often do not understand the Bluetooth technology."

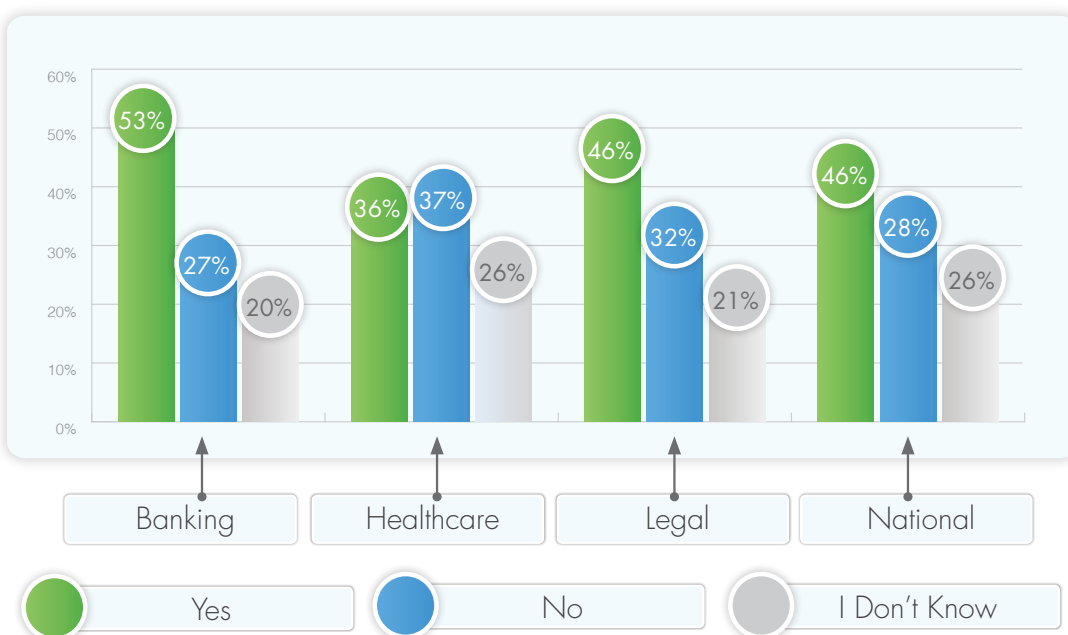
Mobile security breaches are still rare, but with a full-time workforce of about 115 million Americans toting at least 50 million smartphones, lapses are inevitable.

If a security issue were to arise, 86 percent of workers say their employers can't remotely wipe their device's data. That includes if the device is lost or stolen. As most devices are privately owned, this isn't surprising. However, given the fact that so many smartphones are used for work purposes, this could prove problematic.

Skepticism about this influx of smartphones isn't limited to just employers. Just 42 percent of employees who use personal smartphones for work feel their employers are prepared for problems that could arise from their use.

Industry Readiness for BYOD

Do you feel your employer is prepared for problems that could arise from Bring Your Own Device policies?



Sensitive Industries

Smartphone Security Practices

Personal smartphone usage at work varies within so-called “sensitive industries,” or sectors that come with greater expectations of privacy and security. Those industries for the purposes of this study included healthcare, legal and banking sectors.

Is your smartphone password protected?				
	Healthcare	Legal	Banking	National Average
Yes	59%	64%	67%	60%
No	41%	36%	33%	40%

Do you access unsecured or unknown Wi-Fi networks with your smartphone?				
	Healthcare	Legal	Banking	National Average
Yes	53%	64%	60%	50%
No	44%	36%	40%	50%
I don't know	3%	--	--	--

Do you have Bluetooth discoverable mode disabled on your smartphone?			
	Healthcare	Legal	Banking
Yes	52%	61%	53%
No/I don't know	48%	39%	47%

Interestingly, workers in the legal, healthcare and banking professions don't have markedly higher standards for smartphone security.

Password protection varies by around 6-7 percent within these sensitive industries, which all hover at or are slightly above the national average of 60 percent of workers.

Password protection is a relatively simple practice to enforce when companies requisition and secure their own fleet of devices. It clearly gets harder when it's employees' own smartphones. 40 percent of work devices without passwords is untenable.

Passwords aren't the only basic security practice BYODers tend to eschew. Somewhat greater numbers of workers in sensitive industries reported accessing unsecured wi-fi networks in public places, a well-known security vulnerability.

Conclusions

A Final Thought

The number of Americans with smartphones is steadily increasing. Adults who reported owning a device they classified as a smartphone jumped 12 percent in 2012 according to the Pew Center. As that number grows and more Americans return to the workforce in the recovery from this Recession, BYOD will cause security breakdowns and cost companies money.

Knowing some of your employees' smartphone habits can help you prepare to mitigate the impact of those events.

Methodology

The group of Cisco partner firms conducted the study using a randomized, online sampling of full-time American workers. The group analyzed 1,000 responses. The survey population for Americans employed full-time who own a smartphone is roughly 53 million, according to the Bureau of Labor Statistics and the Pew Internet & American Life project. The margin of error of the study is 3 percent.

About the Authors

A network of Cisco IT channel firms collaborated to sponsor this study. These firms help resell and service Cisco products to organizations throughout the United States.

City Appendix

Although not quite a rule, there is certainly a trend of larger markets offering stipends for smartphones more frequently. If you work in Dallas, you're most likely to receive a smartphone stipend. Louisville employers were least likely to offer recompense for smartphones.

Below are 8 markets with statistically relevant sample sizes.

Do you use your personal smartphone for work purposes? Do you receive a stipend for it?		
	BYODers	Stipends
New York	91%	11%
Los Angeles	90%	11%
Chicago	88%	10%
Dallas	91%	17%
Atlanta	89%	8%
St. Louis	88%	12%
Tampa	85%	5%
Louisville	88%	4%